RE: ACCIDENT AT SMILER ROLLERCOASTER, ALTON TOWERS, 2nd JUNE 2015

EXPERT'S REPORT

October 2015

PREPARED AT THE REQUEST OF THE HEALTH AND SAFETY EXECUTIVE

CONTENTS

	Page
Report author	3
Instructions and documents supplied	4
Factual Summary	5
Commentary	7
Conclusions	28
Declaration	30
Appendix 1 – List of Statements provided	33
Appendix 2 – List of Documents provided	34
Appendix 3 – HS(G)175	35
Appendix 4 – Safety of amusement devices: design	36

REPORT AUTHOR

1) I am Stephen Flanagan, trading as 'Stephen Flanagan, Consultant', of [redacted] I provide technical and para-legal support in matters arising under Health and Safety Law, plus expert opinion in matters within my field of expertise.
2) Between 2002 and 2013, I was employed as a Principal Inspector of the Health and Safety Executive (HSE), based at their Newcastle under Lyme office. I joined HSE as an Inspector enforcing occupational health and safety law in January 1990. I hold a Postgraduate Diploma in Occupational Safety and Health. I have attended training courses in Safety Engineering and Ergonomics.
3) Between 1990 and 2013, I was responsible for regulation of a wide range of private and public sector industries. As an Inspector, this was by direct inspection and investigations within those industries, and later as a Principal inspector, largely by management and supervision of Inspectors exercising that role.
4) For a period of approximately 15 months from 2008 to 2009, I performed the role of Head of Operations for the West Midlands area of HSE's Midlands Division.
5) I inspected fairgrounds and amusement parks, and investigated fairground accidents and incidents between 1991 and 2013. I have headed a national team of HSE

Inspectors specifically tasked with conducting audits of the inspection bodies operating under the Amusement Devices Inspection Procedures Scheme (ADIPS).

6) Prior to, and during the whole of my time as a Principal Inspector, I had management responsibility for the activities of the HSE Midlands Division members of the National Fairgrounds Inspection Team (NFIT), and have provided support to NFIT nationally. I have delivered extensive training to Inspectors on the topic of fairground safety, over a number of years. I have delivered a number of Seminars on fairground safety to the fairgrounds industry. I have been consulted on the content of HSE's published guidance for the fairgrounds industry, in particular, HSE publication HS(G)175, 'Fairgrounds and Amusement Parks: Guidance on safe practice' (HSG175). A copy of this guidance is contained in Appendix 3 of this report.

7) I have provided, and continue to provide, expert opinion in relation to a number of prosecutions following incidents in the fairgrounds industry and other industries.

INSTRUCTIONS AND DOCUMENTS SUPPLIED

8) I have been provided with the following documents:

   i. Copies of Statements as listed in Appendix 1 of this report.

   ii. Copies of Documents as listed in Appendix 2 of this report.

9) My instructions, by contract dated 8th October 2015, are to give my expert comment upon "the systems of work and the supporting arrangements for providing information, instruction, training and supervision to relevant staff operating the Smiler ride on and before the 2nd June 2015 at Alton Towers". I have been

particularly asked to "consider the information provided, so as to form opinion on the level of compliance with established benchmarks, including the assessment of risks and commensurate measures for the control of those risks."

FACTUAL SUMMARY

10) The Smiler rollercoaster was in operation during 2nd June 2015, under the control of [redacted], a designated operator of the ride. Shortly after 13.00hrs, she became aware of a slow flashing warning light on the ride's main control panel, indicating a 'fault' condition. Guests were removed from the ride, and she called for assistance from 'Technical Services'. [redacted] and [redacted] mechanical engineers, attended from close by. [redacted] dealt with the fault by moving the key-controlled mode switch from automatic (mode 3), to 'maintenance', or manual (mode 2), and acknowledging or 'clearing' the fault code, thus re-setting the control system to its normal running condition.

11) [redacted] and [redacted] had earlier been told that the Smiler would need a fifth train adding to the track, in addition to the four it had been operating with that morning, because of visitor numbers. [redacted] then decided that there was the opportunity now, whilst no passengers were on the ride, to put the additional train onto the ride. [redacted] informed central 'Control' that the fifth train was to be added. During the process of adding a fifth train, it became necessary to send an empty train around the track. This was dispatched, but after leaving the first lift and progressing along the first, long, unpowered section, it failed to engage properly with the second lift. The main control panel indicated a 'block fault', i.e. the ride's control system

had registered that a train had failed to clear the track section between the first and second lift.

12) [redacted] and [redacted], electrical engineers, arrived at the ride, and began to assist. They were not aware that a fifth train had just been added to the track.

13) [redacted] and [redacted] went out to the train at the second lift, to push it on into the lift chain mechanism. [redacted] in communication with them, operated the control panel in manual mode, and the car was successfully sent on through the ride track, with the result that all cars were now back in the station or waiting areas.

14) [redacted] then sent one empty train up the first lift, in order to establish that the ride was now operating normally. Unknown to those present, this car failed to clear a loop on the section of track between the first and second lifts, and rolled back, coming to rest in one of the track 'valleys'. The ride was then handed back to the control of [redacted] who began to load the first passengers. The first loaded car was sent to the top of the first lift, which triggered a 'zone stop' alarm on the control panel. [redacted] and [redacted] then resumed control. [redacted] identified the positions of the four trains which he believed were on the track by studying the control panel, then went out to the satellite control panel out on the track, close to the foot of the second lift. There was no train present at the foot of lift 2. He failed to notice the stalled train in the track valley. His function was to press a button on that control panel, simultaneously with [redacted] pressing of a button on the main control panel, which would clear the 'zone stop'. This was done, the consequence being that

the control system would no longer regard the section of track between the first and second lifts as being occupied.

15) [redacted] then asked central 'control' for a 'Code Zero' permission, which would enable her to operate the ride in 'mode 4', i.e. evacuation mode. This would command the control system to systematically return all trains to the station, beginning with the train most advanced through the track, and working backwards. With permission granted, she began the process. In accordance with the programmed logic of the evacuation mode, the control system began by moving the train which it believed was furthest through the ride sequence, i.e. the train loaded with passengers held at the top of lift 1. This was sent on, and crashed into the stranded car in a 'valley' between the two lifts.

COMMENTARY

Safety at Fairgrounds

16) The operation of fairground rides is generally considered to be a high hazard activity. That is to say that an untoward event such as the one occurring on the Smiler ride would potentially have serious consequences, involving serious multiple injuries or fatalities. In such situations, it is important that the risk, or likelihood, of such an event actually occurring is reduced to the lowest degree reasonably practicable, and a higher level of precautions would generally be expected than in situations of low hazard, i.e. where any harm which materialised would be minor.

17) In recognition of this, HSE has worked with the industry to produce detailed guidance on the precautions to be taken. The main guidance is set out in HSG175.

18) HSG175 sets out a 'System for safety of attractions', consisting of a series of 'steps' and 'checks' intended to ensure safety from design of a fairground ride, through to the ride's operation and maintenance. This can be found in tabular form (table 1) on page 7 of HSG175. The requirement for 'checks' is intended to avoid the situation where defects, faults and errors are not detected. I consider that this is consistent with the usual goal of a Safety Engineer, which is the avoidance of conditions where a single failure (whether a 'hardware' failure or a human behavioural failure) leads directly to a high hazard situation without opportunity for intervention or correction.

19) HSG175 is written as generic guidance, but it does point towards issues which are relevant to the matter under consideration, with some very basic advice. At paragraph 252 it states *"General information and training for all employees involved in running a device need to cover at least the following areas: .....how to deal with defects and malfunctions"*.

20) The approach by HSG175 of requiring steps and checks can be illustrated with the example of ride design. The requirement (or 'step') in table 1 is for design *"by competent designers with knowledge of the relevant standards"*. The additional requirement is for an independent **check** on the soundness of the overall design concept, by the process known as 'Design Review'. HSG175 goes on to provide advice on design under the heading of 'Design risk assessment (DRA)', at paragraphs 34 and 35. These state *"The fairground industry publication 'Safety of amusement devices: Design' defines a design risk assessment as: 'the process of assessing the hazards that an amusement device might pose, the likelihood of those hazards posing a risk and the control measures that are necessary to control those risks adequately.*

As a fundamental element of the design process, you should assess all the risks associated with the design, as well as those risks arising out of the activities specified in paragraph 29 and record this in the DRA. It should be used to help specify the safety functions of the amusement device". Paragraph 29 refers to the need for the design to aim to ensure safety during assembly, dismantling, transport, installing, operation, cleaning, maintenance, inspection, testing and use by the public.

21) The joint ADIPS/HSE publication 'Safety of amusement devices: Design' (SADD) gives detailed guidance on the conduct of a Design Risk assessment, and at chapter 9, paragraph 15(g), emphasizes the value of use of analytical techniques such as 'Failure Modes and Effects Analysis', as part of the design risk assessment process. A copy of SADD is attached to this report at appendix 4.

22) Failure Modes and Effects Analysis (FMEA) is widely used in the design of complex plant and machinery in high hazard situations. It considers the many ways in which plant or machinery may go wrong, and the consequences of such failure, and seeks to identify means of ensuring that such failures do not lead to immediate danger.

23) FMEA is founded upon the use of a number of fundamental principles used by the safety engineer. I would summarise the key principles as:

i. Redundancy. It is the nature of many components of a device, for example, a fairground ride, that the failure of a single component will occur at random. If the component selected has an acceptably low random failure rate, then a high level of safety integrity can be introduced simply by doubling up the provision of the key component, in a design where either of the two components, if functioning, can maintain safety independently. A simple example of this

from everyday life would be the introduction of 'dual-circuit' brakes on motor cars. With this development, safety was no longer reliant on a single hydraulic circuit.

ii. Diversity. This principle recognises that situations can exist where two or more device components which apparently operate independently of each other, may both be affected by the failure of some other element of the design. Returning to the example of motor car brakes, even if a dual circuit system is fitted, a failure to maintain an adequate supply of brake fluid in the reservoir, or the loss of containment of the reservoir (e.g. a leak), could lead to the non-functioning of both hydraulic circuits, and complete loss of braking. This type of failure is referred to as 'common mode' failure, or 'systematic' failure. The safety engineer's solution to this problem is normally to introduce additional components or systems which do not rely upon the same aspects of the design for their continued function. This is the principle of diversity. The motor car braking example would be that in addition to the hydraulic footbrake, a cable-operated handbrake is also provided, which is not reliant upon the hydraulic system.

iii. Failure to Safety. If the design can be arranged such that failure of key components will be a failure to a safe condition, then this will amount to inherently safe design. A motor vehicle example would be the braking systems of Large Goods Vehicles, which are air/spring systems, and can be described as 'air off, spring on', such that loss of the air supply leads to the brakes locking on, rather than loss of braking functionality. Good design may

also include provision for faults to be self-revealing. Taking the example of two identical components, with an acceptable random failure rate, these will normally be arranged such that either of the components can independently maintain safety. However, if the design does not lead to the initial fault being revealed, then the device will continue to function with one failed component, hence no redundancy, until the second component fails to danger. In complex designs, it will often be necessary for the device's control system to include some form of monitoring of the condition of safety critical components, in order to deal with this issue.

iv. Hierarchy of control measures. Another fundamental principle is that of selecting inherently more reliable control measures or components over those less reliable. A general rule adhered to is that properly designed and constructed hardware control measures will be inherently more reliable than reliance upon human actions. For example, it is understood that adequate physical guarding of dangerous parts of machinery is inherently more reliable than issuing instructions to workers to 'keep your hands out', or the like. Therefore, in situations where it is necessary to rely on human actions in high hazard systems, it is all the more vital to apply the safety engineer's principles of redundancy, diversity, and failure to safety to the systems of work which need to be created to direct human actions.

Safety of Rollercoasters

24) The principles of safety engineering which I have outlined above have been successfully applied to the design of fairground rides, probably most notably in the

case of rollercoasters. Whereas the public perception of the hazards associated with rollercoasters may be focused on the danger of a train parting company with the track, in reality, the bigger, and more difficult to resolve issue has always been the hazard of trains colliding on the track.

25) Considerations of 'throughput', (numbers of riders passing through the ride) have tended to lead to designs which can operate with multiple trains sharing the track. This can only be achieved safely if the ride is operated to a 'block system', where conceptually, the track is separated into sections, or 'blocks' and a control system prevents more than one train ever being in a given block at any one time.

26) In the early years of rollercoaster design, control systems were often rudimentary, and involved a large degree of human input for their functioning. For example, the collision accident at Battersea Park, London which killed five in 1972 occurred on a wooden rollercoaster which required manual braking under the direct control of a ride attendant. With increasing complexity, control systems have become more sophisticated, and are now almost universally not primarily reliant on human intervention.

27) Following a period of control system design which relied upon 'hardwired' relay-logic systems, there is now an almost universal reliance upon computer based control systems, because it produces a cheaper, more compact solution.

28) Conceptually, a well-designed system, would incorporate the design principles which I have set out above. The system will be designed around Programmable Logic Controllers (PLC). These are specialised computers, with a high degree of initial integrity. Redundancy is generally achieved by configuring the control system to

incorporate, conceptually, two discrete channels of control. This may require the use of two PLCs, and each of the safety critical input devices providing information to the PLCs will be doubled up. Typically this will involve proximity switches detecting the entry and exit of trains from sections of the track being provided in pairs. Each of the pair will provide an input into one of the channels of control. It is recognised that computer software is prone to 'systematic failures' i.e. faults which will always materialise under particular conditions, and so the use of dissimilar software in each channel of control, or the Quality Control of software, is common. Further, 'failure to safety' is generally ensured by a constant 'cross-monitoring' between the two channels of PLC control, which will detect any difference in status between the two channels of control, and shut the ride down to a safe condition. Good control system design will also recognise the advice contained in Chapter 1 of the SADD guidance, at paragraphs 47 and 50, when considering an appropriate hierarchy of control measures.

29) Paragraph 47 states *"Training, and experience might reduce the risk but none of these factors should be used as a substitute for risk reduction by design or safeguarding where such safety measures can be reasonably practicably implemented. Due to the exposure of large numbers of members of the public, inappropriate reliance should not be placed on ride operators/attendants having to develop an unreasonable degree of skill or acquired knowledge to ensure public safety".*

30) Paragraph 50 states *When safety measures include:*

a. *work organisation,*

b. *correct behaviour,*

c. *diligence,*

d. *application of personal protective equipment,*

e. *skill or training,*

the relatively low reliability of such measures, as compared to proven technical safety measures, should be taken into account in the risk estimation. Where it is reasonably practicable to employ technical and or physical safety measures this should be done in preference to relying on those measures listed above.

31) The SADD guidance also provides further advice on the limitations of reliance on human actions as a means of ensuring safety, by reference to 'Human Factors', in paragraphs 45 and 46 of Chapter 1. Paragraph 45 states, *"Human Factors can affect risk and shall be taken into account in the risk estimation. This includes, for example:*

a. *Interaction of persons with the amusement device;*

b. *Interaction between persons;*

c. *Psychological aspects;*

d. *Ergonomic effects;*

e. *Capability of persons to be aware of risks in a given situation (e.g. in relation to ride operators or maintenance staff) depending on their training, experience and ability.*

32) Paragraph 46 states, *"The estimation of the ability of exposed staff shall take into account the following aspects:*

a. *Application of ergonomic principles in the design of the device;*

b. *Natural or developed ability to execute the required tasks;*

c. *Awareness of risks;*

d. *Level of confidence in carrying out the required tasks without intentional or unintended deviation;*

e. *Temptations to deviate from the prescribed and necessary safe working practices.*

The design of the Smiler rollercoaster

33) When commenting, in line with my brief, on the adequacy of the systems of work in place for operation of the Smiler ride, it is worthwhile considering initially whether the ride design was adequate, when assessed against the above mentioned criteria as applied by safety engineers.

34) The literature supplied to me which originates from the manufacturer, Gerstlauer, does not contain a comprehensive description of the control system for the Smiler. However, there is mention of an 'Allen Bradley' PLC. I am aware that this is a reference to a manufacturer of a type of PLC much favoured by rollercoaster manufacturers. Exhibit LM/47f, an Alton Towers risk assessment for ride maintenance, identifies the PLC as being 'dual process'. Based on this, there would appear to be a control system providing two separate channels of control.

35) Exhibit LM/21 'Infinity Coaster the Smiler Original Operating instructions', provides a brief description of the 'block system', at page 57. This document is clearly a

translation from the original German, with the limitations of that, but I derive the meaning from it as i) entry of a train into a block is monitored by a pair of proximity switches, and a signal from at least one of the switches is sufficient for the control system to regard the train as having entered the block, and ii) exit of a train from a block is monitored by a pair of proximity switches, and a signal from both of the switches is required for the control system to regard the train as having left the block. This demonstrates the correct approach to ensuring safety through 'redundancy', using 'AND' and 'OR' logic in the control system appropriately, i.e. OR logic for situation i) above, and AND logic for situation ii) above.

36) From this, and consideration of the witness statements of ride operators and Technical Services engineers, I conclude that the control system appears to have the necessary attributes to allow the ride to be run safely in an automatic mode, under normal conditions.

37) It is also apparent that the ride designers have applied the principles of safety engineering and the science of Ergonomics to the interface between the ride control system and its human operators, and have paid due regard to the provisions of the SADD guidance, chapter I, paragraphs 47 and 50 as referred to above, by seeking to limit the potential for human error.

38) The first example of this which I cite is the configuration of the control system regarding the arrangements for loading passengers into trains in the station. Ensuring that passenger restraints are properly closed is safety critical, and I note that the usual modern convention of monitoring the position of each restraint, and providing an input to the control system, is followed. This, together with a physical check by ride

attendants (as required by HSG175, and introducing redundancy and diversity) largely eliminates the possibility that a passenger could ride without the restraint being locked. However, the need to physically check restraint locking brings the ride attendants into close contact with the train. The consequence of a train being dispatched prematurely in those circumstances could be serious, in terms of injuries to ride attendants. Hence, dispatch is only allowed by the control system if it receives simultaneous inputs by button pressing by the ride attendants and the ride operator. This largely eliminates the possibility of the ride operator dispatching a train prematurely, i.e. once the restraints have locked, but before the attendants are clear of the train. This builds in a second layer of control measure, using the 'AND' logic principle.

39) The second example I cite is of the control system configuration relating to the 'clearing' of block faults. This ride will indicate a block fault in the event that the signals received for relevant proximity switches indicate that a train has failed to exit a block. Because the control system does not, and cannot, have eyes, the signals from the proximity switches are a proxy for reality, and may not always accurately reflect reality, and so it is designed to err on the side of caution. This can be regarded as an application of the concept of 'failure to safety'. Therefore, in order for the system to safely restart, human intervention is necessary. A person or persons must satisfy themselves that the relevant block is empty or has been emptied. This ride's control system has been configured with satellite control panels at suitable locations around the track. It is necessary for the person in charge of the main control panel, and a second person located at the relevant satellite control panel, to press buttons

simultaneously. The thinking behind this requirement seems to be that it requires a person to physically visit the area of the block to be 'cleared' thus encouraging the necessary visual check. This is reinforced by the manufacturer's supplied literature pointing out this need. Without this, there is the danger that persons may rely too much on the indications of the rides condition as shown on the main control panel, which does not always represent reality; or, as occurred in this accident, there could be undue reliance on an unconfirmed presumption (in this case as to the number of trains on the track).

40) The third example I cite is the provision of an 'evacuation' mode, selectable via the mode switch located on the main control panel. When, for breakdown or maintenance purposes, it becomes necessary to take all passengers off the ride, the use of the automatic running mode is not appropriate, because it would continue to send cars around the track, and reaching the desired end result of all the cars being empty in the station area could be difficult to achieve. The evacuation mode provides a relatively straightforward means of achieving the evacuation simply and quickly, with the minimum potential for human error. It represents good design. However, the safe use of the evacuation mode is dependent on the proper following of the procedure for clearing block faults, as I have described in paragraph 39 above. If the control system is not aware of the true position of all trains, it cannot operate the evacuation procedure safely. This is central to the immediate causes of the accident on the Smiler.

41) In summary, the Smiler ride appears to me to be a well-designed ride which has been through a process of design review, as evidenced by exhibit LM/32 'Declaration of

Operational Compliance'. Its design incorporates features designed to limit the need for human intervention during operation, and thus to reduce the potential for human error. The design also recognises the limitations of human actions as a control measure, and follows sound ergonomic principles by providing a person/machine interface which encourages informed decision taking which relies on more than one individual acting alone.

Operating Procedures for the Smiler Ride

42) However well a rollercoaster may be designed, with current technology, significant human intervention will be required, and it is vital that this is done safely.

43) This issue is addressed by the science of Ergonomics, which is often expressed as the science of 'person centered design'. Such design has obvious benefits related to usability, efficiency, and the minimising of the potential for error. A very simple example would be the fact that it is now almost universal that the direction indicator control on motor cars has been standardised to a stalk to the left hand of the steering wheel. This has improved the likelihood that a motorist will give a correct signal at the appropriate time (rather than operating the windscreen wipers), particularly when driving an unfamiliar car.

44) In the work environment, much attention is given to situations where individuals have to perform complex tasks, because of the raised potential for human error. Control measures can include careful design of the person/machine interface (for instance the provision of a 'mimic' or graphic display showing the status of the Smiler ride), realistic design of the task which avoids overburdening the worker, and the use of a technique commonly referred to as 'Task Analysis'.

45) Task Analysis attempts to review, define, and standardise procedures. In the language of industry generally, it can be expressed as the laying down clear and defined systems of work. Where such systems are safety related, they can properly be called 'safe systems of work', as required by the Health and Safety at Work etc. Act 1974. Task Analysis is achieved by breaking down the required task into its component parts, ordering them in safe and efficient sequence, and making provision for actions to be taken in the event of foreseeable deviations from the norm by any plant or machinery being worked with. Typically, clear and emphasised 'do's' and 'don'ts' will be included. Workers would be trained in the procedure, step by step, and their understanding and capacity to follow the procedure tested. Where safety critical steps in the process are identified, it is common in high hazard situations, to introduce checks on actions, to confirm the absence of error.

46) The routine operation of the Smiler ride is in the hands of staff employed in the Operations Department at Alton Towers. The key document which illustrates the systems of work which they operate to is exhibit LMS/04 'The Smiler Cabin Folder'. This contains the document 'Code of Safe Working Practice – The Smiler 2015'. It is a large document, which reflects the degree of complexity of the task of a ride operator. I consider that it bears the hallmarks of having been produced as a result of a process of Task Analysis. It carefully details the sequences of all the processes or work activities which a ride operator is expected to perform, and puts clear limits to the actions which they are authorised to perform. It is evident that the main limitation placed on operators is the requirement to call in, and pass over control of the ride, to the Technical Services Department in the event of the ride control system indicating a

'fault'. This is a sensible separation of function, because it reduces the overall complexity of task which any one individual has to face, though it brings with it the challenge of the need for effective communications at handover. I note that a ride log was in use on the ride, which could have assisted in this.

47) The documents provided which relate to the training of ride operators, i.e. exhibit LM/33, indicate training and assessment which closely follows the format and content of the Code of Safe Working Practice for the Smiler. There also appears to be ongoing re-assessment of ability to follow the systems of work, at the start of each operating season.

48) In summary, I am reasonably satisfied as to the adequacy of the systems of work, training and on-going supervision of Operations staff, subject to one qualification. This is that the procedures permit the Operator, on receiving control back from Technical Services, to ask 'Control' for permission to undertake a 'Code Zero'. This would be switching the ride into evacuation mode, which is a safe procedure only if the ride control system has an accurate understanding of the location of all cars. The granting of that permission appears to have been a mere formality, with the opportunity to double check the safety of the proposed action lost. Having said that, it should have been possible for Technical Services department to perform such a double check. What remains unacceptable is for nobody to perform an effective double check.

49) The arrangements in place for Technical Services staff (the engineers) are in sharp contrast to those in place for Operations staff.

50) There is no evidence of a structured Task Analysis based approach to their work, though I hold the view that such an approach would be readily achievable, particularly in relation to the safety critical task of dealing with ride 'faults'.

51) Whenever the Smiler ride displayed a 'fault' it was vital that the appropriate checks were diligently made, so as to bring the ride to a safe condition without harming passengers. This was a process which could have been defined, via Task Analysis.

52) The documents supplied indicate a quite different approach by the Technical Services Department. Training tended to be delivered by observation of and working with, existing engineering employees. Such an approach is not systematic, and tends to pass on bad practice as well as good. It also leads to staff with varying degrees of knowledge, and inconsistent beliefs. For instance, [redacted] electrical engineer, states, '[redacted]" He also states '[redacted]

The emphasis in the department was upon skills, experience, competence and qualifications. This would be commendable if it were the case that such attributes in a person guaranteed the absence of errors. If that were the case, there would be little or no need, for example, for:

i. Systems of work in hospital operating theatres designed to 'count in' and 'count out' the numbers of swabs and instruments used, in order that surgeons do not leave them inside patients,

ii. Co-pilots double checking the actions of pilots in civil aircraft,

iii. Independent Design Review of the fairground ride designs of competent ride designers,

iv. Guards, on machinery being operated by skilled and qualified engineers.

53) In my opinion, there were factors present at the time of the accident on the Smiler ride on 2nd June 2015, which were avoidable, and which contributed to causation of the accident:

i. There was no single member of the Technical Services Staff who was required to take, or took, overall control of the process of bringing the Smiler ride safely back into service. Four members of Technical Services Staff, and one

operator had varying degrees of input into the process, and none of had a full picture or understanding of the condition of the ride, and what was required for safety.

ii. There were various states of knowledge as to the significance of fault alarms generally, and block faults in particular.

iii. The inadequate state of knowledge of Technical Services staff led to distrust of the otherwise clear fault signals being received from the ride control system. The belief appears to have been formed that that the control system was unreliable, and that their own judgement and decision taking was inherently more reliable. This was perhaps founded upon a failure to appreciate that the control system was of sound design, but was quite correctly designed to 'err on the side of caution' (given that it has to rely entirely on input from sensors, and does not literally have its own eyes). This would inevitably lead to numerous apparent 'false alarms'. The problem then arises that where individuals lack hard rules of behaviour as would be provided by a written system of work, they tend to become habituated to false alarms, and tend to assume that all alarms will be false. (It is understood in the science of Ergonomics that careful design of complex control panels for high hazard applications requires the judicious use of alarms. An overabundance of alarms for minor conditions may 'de-sensitise' operators to alarms generally, i.e. the 'cry wolf' syndrome)

iv. The Technical Services staff were filling in for the gaps in their knowledge with assumptions. Maintenance engineers have to be good fault finders.

There may be limits to what testing can achieve, therefore, some of their fault-finding activity will to be based on making reasonable but unproven assumptions. This is a common technique which is generally effective. If an error is made, the only consequence is usually the need to make fresh assumptions and begin the process again. However, it has no place in a safety-critical situation. There has to be a strict 'deductive' approach of reasoning from demonstrably known facts, to a conclusion. The process might go: 'i) the ride is only safe to operate again if there are no trains in any track blocks, ii) There is clear and confirmed visual evidence that no trains are in track blocks, and iii) therefore, it is safe to operate the ride. This deductive logic can be provided in a suitable written safe system of work.

v. There was no formal control over who was entitled to clear particular faults, or the checks which should be done before clearing them.

54) In consequence of the factors mentioned above, a number of human errors occurred:

i. Error no. 1. The mechanical engineers, [redacted] and [redacted] took the opportunity to load a fifth car onto the track, but failed to communicate effectively, and verify that the electrical engineers, [redacted] and [redacted] understood this, even though they were aware that [redacted] and [redacted] were dealing with a fault. [redacted] states that he told [redacted] whereas [redacted] states "[redacted] and [redacted] states '[redacted] This could usefully be classified as a 'communications' error.

ii. Error no. 2. [redacted] AND [redacted] made assumptions about the number of trains on the ride, without directly verifying it. Although an entry was made in the ride log indicating the addition of the fifth car, neither [redacted] nor [redacted] looked in the log, perhaps unsurprisingly, given that there was no formal written procedure to require them to. Human Factors Ergonomists would tend to classify this error as a 'misperception'.

iii. Error no. 3. When a second block fault occurred between lift 1 and lift 2, it indicated that a train at the top of lift 1 was not being allowed to move into the next section of track. [redacted] states '[redacted] This appears to be another 'misperception', based on poor knowledge of the ride. It appears to me that the error message was indicating that the control system considered the block to be occupied by a train, but because of the previous errors which led to the failure to identify the presence of a fifth train on the track, a false assumption was encouraged. The opportunity to use the CCTV monitors to look at all of the relevant section of track was lost, with [redacted] concentrating solely on the area at the foot of

the second lift. Thus, [redacted] was now satisfied that it would be safe to do a block re-set. This could not in itself have led immediately to danger, because of the hardware precautions built into the ride design, which require simultaneous pressing of buttons by two persons.

iv. Error no. 4. [redacted] went out onto the track in order to press the relevant button on the satellite control panel adjacent to the foot of lift 2. The ride designer's intention was that any person pressing that button should have first established beyond doubt that the track section was free of any train. The Gerstlauer 'Original Operating Instructions' (exhibit LM21) state, at paragraph 4.11.3 'Brake Operator Panel 1 – B01 &B03' *"In case of a wrong block occupancy, e.g. after a shut down, the block at the brake can be reset by the panel at the valve box. This can be necessary, if the block is already occupied while no train is present at the block. This case prevents an advancement of the train in the previous block. The responsible person must make sure that there is actually no train present"*. The obvious way to do that was by direct visual observation. However [redacted] had already satisfied himself as to the position of **four** cars. He states '[redacted]

[redacted]' Having made this mistaken assumption, [redacted] went out to the trackside satellite control panel. He states [redacted] This suggests that [redacted] error could also be regarded as based upon 'mistaken priorities'. It is clear that his priority had become getting the ride quickly back into service, and he felt pressure to that effect. The evidence provided to me also indicates that management had set targets for downtime on rides, with bonuses linked to achieving acceptably low levels. There were also 'clocks' in the ride control cabins showing the current performance on downtime.

CONCLUSIONS

55) The Smiler rollercoaster was designed to current standards, and had a sophisticated control system and an ergonomically sound user-interface for operators.

56) The arrangements (system of work, training and supervision) put in place for ride operation by the Operations department were based on sound safety engineering principles, and provided an adequate basis for safe operation in 'normal' mode.

57) The Technical Services department either failed to recognise the safety critical nature of the task of dealing with faults to the ride, or else lacked the safety engineering expertise to devise systems which would deal with the inherent unreliability of relying on human actions in a safety critical situation.

58) The consequence of the Technical Services department's failings was that a situation arose where serious error was a potential outcome, and that outcome materialised.

59) I consider that the additional precautions (which are not intended to be prescriptive, as other similar arrangements could be equally effective) which I have indicated ought to have been taken are eminently reasonably practicable. These suggested precautions are in my report above, and at paragraph 61 below. To a great extent, the reasonably practicable nature of the suggested precautions is illustrated by the fact that the Operations department had such precautions in place, covering a similar situation. Further, since the accident, the Technical Services department has written exhibit LM/56 "Engineering Code of Safe Working Practice The Smiler 2015", which puts such arrangements in place. In addition, the items of correspondence and submissions to HSE relating to compliance with the Prohibition Notice issued for the ride, suggest an ability to devise suitable precautions.

60) Much of the documentation supplied to me which emanates from Alton Towers suggests an organisation which has a well-developed system for safety management, with evidence that monitoring and audit went on. Therefore, I am concerned that

senior management appears never to have become aware, or failed to act upon, the great discrepancy between the robust arrangements put in place by the Operations department and the manifestly inadequate arrangements of the Technical Services department. My recommendation would be that Alton Towers should review the adequacy of its audit arrangements.

61) I am satisfied that if the Technical Services Department had devised a formal written system of work based on Task Analysis and Safety Engineering principles, had trained its staff and monitored their performance to similar standards to those of the Operations department, it is very likely that this accident would have been avoided. Key features of such a system of work could be:

i. One suitable individual should always be appointed or nominated as being in charge of the activity of bringing the ride safely back into use, directing all activity, following a fault condition.

ii. Key decisions potentially affecting the safety of the ride, and requiring formal confirmation of the status of the ride should always be based upon decisions by at least two persons, operating to 'AND' logic, thereby introducing redundancy, and should always be based upon direct observation (thereby reducing the possibility of a common mode failure, i.e. a shared misperception).

DECLARATION

62) I declare that,

i. I understand that my overriding duty, both in preparing reports and in giving oral evidence, is to provide independent assistance by way of objective,

unbiased opinion. I confirm that I have complied with, and will continue to comply with that duty;

ii. I have endeavored in my report and my opinions, to be accurate and to cover all relevant issues concerning the subject matter that I have been asked to address. The opinions expressed represent my true and complete professional opinion;

iii. I have endeavored to include in my statement those matters which I have knowledge of and of which I have been made aware, which might adversely affect the validity of my opinion;

iv. I have indicated the sources of all information which I have used;

v. I have where possible formed an independent view on matters suggested to me by others including my instructing lawyers and their clients; where I have relied upon information from others, I have so disclosed in my report;

vi. I will notify those instructing me immediately and confirm in writing if, for any reason, my existing report or opinion requires any correction or qualification;

vii. I understand that my report, subject to any corrections before swearing as to its correctness, will form the evidence which I will give under oath;

viii. I understand that I may be cross-examined on my report by a cross-examiner assisted by an expert;

ix. I understand that I am likely to be the subject of public adverse criticism, if the court concludes that I have not taken reasonable care in trying to meet the standard set out above;

x. I confirm that I have not entered into any arrangement whereby any of my fees are in any way dependent upon the outcome of this case.

Appendix 1 – List of Statements provided

Appendix 2 – List of Documents provided

Appendix 3 – HS(G)175 'Fairgrounds and Amusement Parks: Guidance on Safe Practice

Appendix 4 – 'Safety of Amusement Devices: Design